Abstract: A Zero-Knowledge protocol is an interactive protocol between two parties in which one party, called the prover, wants to prove to another party that he/she knows a secret, without revealing the secret information itself. Existing Zero-Knowledge protocols require heavy computations, derived from complex mathematical formulations. On the other hand, Visual Cryptography is a special cryptographic technique used to encrypt and decrypt visual information with the human eye without the aid of computers. This research proposes a new scheme of Zero-Knowledge Proof of Identity based on visual images. The proposed scheme is a combination of the concepts from Visual Cryptography and Zero-Knowledge schemes to utilize the advantages of both techniques. The proposed scheme starts when the prover sends a request to the verifier. The verifier replies with an image as a challenge to the prover. Consequently, the prover sends a response based on the challenge image. The security of the proposed scheme is assured by a hard mathematical problem and hash function. The performance analyses show that, the proposed scheme performs equally well compared with existing visual zero-knowledge schemes. The results show that the proposed scheme is a valuable alternative to existing zero-knowledge schemes where the secret information decryption and verification procedure are performed visually, which is highly user friendly.

Key words: Visual cryptography • Zero knowledge scheme • Information hiding • Communication • Information integrity

INTRODUCTION

In recent times, our world has been characterized by the exchange of data between two parties via public communication networks. In some cases, very important and sensitive data are exchanged through the open network - for example, the use of credit card numbers or passwords to access a secret database. During the process of communication, unwanted consequences may occur if an eavesdropper intercepts the transmission. This third party might use the secret data in some malicious way for personal benefit. Therefore, there is an urgent need to find a solution to the problem of ensuring the integrity of the information. Hence, the idea of proving knowledge without revealing any secret information is very attractive. Zero-knowledge algorithms are based on hard mathematical computations; therefore, verification is performed mathematically. Due, to the fact that humans are visually inclined when processing data, there is a need to design a zero-knowledge scheme based on visual cues. The aim of the new scheme is to reduce the complexity in the zero-knowledge proof identity and to ensure that the verification can be performed visually since the new scheme is based on the concept of visual cryptography, which intern is based on the ability of the human eye to decrypt.

Visual Cryptography: Cryptography can be defined as the art of protecting information by converting it into an unreadable format. Cryptography uses several algorithms that are based on mathematical equations to encrypt and decrypt data. Visual cryptography, a special kind of cryptography that is used to encrypt and decrypt visual information (such as pictures, text, etc.), does not require complex mathematical computations and its decryption process can be performed by the human eye without the aid of computers. Visual cryptography was presented for the first time by Moni Naor and Adi Shamir in 1994 [1].
Visual Cryptography for Black and White Images: There has been a lot of research carried out on visual cryptography for black and white images [2-5]. In visual cryptography for black and white images, the images are encrypted into shares, whereby each share looks like a noisy image. Each pixel in the original image is split into smaller blocks resulting in the same numbers of black and white blocks. If the pixel is split into four parts, the resulting pixel will contain two white blocks and two black blocks in each share as shown in Table 1.

In 1999, a new visual cryptography scheme was proposed for black and white images. The image is encrypted into the same size share of secret image without expansion as shown by Table 2 [6, 7]. To generate the shares in this method, random selections are made in one column, $S_0$ or $S_1$ depending on the color of the pixel. The method assigns $i$-th row of the selected column to $i$-th share, since $S_0$ and $S_1$ are Boolean basis matrices. In this method a new parameter, $B = P_0 - P_1$, is defined to represent the contrast of the recovered image where $P_0$ and $P_1$ are the possibilities that a black pixel created in the image recovered from the black and white pixels in the secret image.

Visual Cryptography for Color Images Scheme: In 1996, Rijmen and Preneel proposed a visual cryptography approach for color images [8]. Young-Chang Hou (2003) in his paper proposed methods for the visual cryptography of gray-level and color images. The first method was the conversion of color image into three RGB or CMY halftone images. Moreover, each pixel in the halftone was expanded into blocks, hence each halftone images is used instead of the original images to get shares. Visual cryptography for color image algorithm works as follows [9]:

- Decomposition the image into CMY halftone images.
- For each pixel $P$, with its components which are $(C,P,M,Y)$ do the following:
  - Select a black mask with a size of $2\times2$ the mask become half white-and-black block as shown in Table 3.
  - Determine the position of $C$ in the first share image. This is done according to the value of $C_i$. If $C_i = 1$, fill the positions of the white color in the mask with a cyan. If $C_i = 0$, fill the positions of the black color in the mask with a cyan. This block will be positioned in share 1.
  - Repeat (b) for M in share 2 and Y in share 2.
  - Repeat Step 2 until every pixel of the composed.
- Stack the four sharing images which is mask. The C share, M share and Y share can be decrypted by the human eye (Figure 1).

Zero-Knowledge Proof of Identity: Zero-knowledge proof of identity is a special cryptographic algorithm for identification and authentication. Zero-knowledge proof is an interactive protocol between two parties, where one party proves to another that he/she has a secret, without revealing the secret information itself. The security of zero-knowledge proof is based on complex computation. A Zero-Knowledge interactive usually takes the form of a three way protocol [10]:

- **Witness**: The prover chooses a random number $x$ and then sends this number to the verifier.
- **Challenge**: In this phase, the verifier chooses a question randomly based on $x$ and sends it to the prover.
- **Response**: The prover sends his/her answers to the questions to the verifier, using his secret information.
Fig. 1: Figure 2.8: Four separating shared transparencies and result of stacking: (a) Share 1(C), (b) Share 2(M), (c) Share 3(Y), (d) Mask and (e) stacked image [9]

Fig. 2: The protocol of zero-knowledge proofs of identity based on the Elgamal on conic scheme

**The Ali Baba’s Cave:** The classic example of cave or Ali Baba's cave [11] is famously used to explain Zero-Knowledge. As shown in Figure 2, there is a circular cave with one entrance referred to as the magic door. The magic door is located inside the cave blocking both opposite ends. Transmission requires the first part, (the prover) to prove that he or she knows the secret word to open the magic door but does not reveal it to the second part, (the verifier). One round of this protocol takes place as follows:

- The prover goes inside the cave and stands in the point of two paths (point Q), while the verifier waits outside.
- The prover chooses path L or R randomly and goes to the magic door. At this time, the verifier moves inside the cave to point Q.
- The verifier alerts the prover to come out and also chooses the random path L or R, where the prover may pass through.
- If the prover knows the secret password to open the magic door, he/she can come through the correct path every time. However, if he does not know the secret password, there is only a 50% probability that he/she can come through the correct path.

The verifier and prover repeat this protocol many times. After many repetitions, the verifier will be convinced that the prover knows the secret word required to open the magic door. If the protocol is repeated t times, the probability that the prover to be cheating is.

**Feige-Fiat-Shamir Zero-Knowledge Proof of Identity:** Uriel Feige, Amos Fiat and Adi Shamir proposed new scheme in their paper, known as the "Feige-Fiat-Shamir
zero-knowledge proof of identity” [10], which is based on the zero-knowledge protocol. This scheme is the best-known zero knowledge proof of identity. The Feige-Fiat-Shamir zero-knowledge proof of identity works as follows:

Initial Parameters:

- A trusted center chooses two large prime p and q and puts n = pxq public modular for all users.
- A trusted center or arbitrator chooses a number v to generate Peggy’s public and private keys where \( x^2 = v \pmod{n} \) has a solution and \( v^{-1} \pmod{n} \) exists.

The Protocol Steps:

- Peggy chooses a random number \( r \), where \( r \) is less than \( n \) and then computes \( x = r^2 \pmod{n} \).
- Peggy sends \( x \) to Victor.
- Victor sends Peggy a random bit, \( b \). The value of \( b \) is either 0 or 1.
- If \( b = 0 \), then Peggy sends Victor \( r \). If \( b = 1 \), then Peggy sends Victor \( y = r^s \pmod{n} \).
- If \( b = 0 \), Victor verifies that \( x = r^2 \pmod{n} \), proving that Peggy knows \( \sqrt{x} \). If \( b = 1 \), Victor verifies that \( x = y^2 \times v \pmod{n} \), proving that Peggy knows \( \sqrt{x} \).

In the same paper, Feige, Fiat and Shamir showed how parallel construction could reduce Peggy and Victor’s interactions and increase the number of accreditations per round [10].

Guillou-Quisquater (GQ) Zero-Knowledge Proof of Identity: The most famous zero-knowledge protocol for identity is Feige-Fišt-Shamir; however, this protocol is based on increasing the number of iterations and accreditations, which is not ideal in some implementations like smart cards. Guillou-Quisquater (GQ) zero-knowledge protocol proposed [12] to solve the main problem of the Feige-Fišt-Shamir protocol by reducing the number of interactions between the prover and the verifier, as well as accreditations per iteration. Guillou-Quisquater (GQ) protocol is based on RSA.

Initial Parameters: The prover in this scheme must choose a bit string of credentials, \( J \), to be used as public key which can be a card ID or bank account number, an exponent \( v \) and a modulus \( n \), which is the product of two primes. In addition, the private key \( B \) is computed so that \( J \times B^v = 1 \pmod{n} \) in which Peggy sends Victor her credentials, \( J \). She wants to prove the credentials are hers, so she must to convince Victor that she knows \( B \).

The Protocol Steps:

- Peggy, the prover sends her credentials, \( J \), to Victor.
- Peggy, the prover selects random \( r \) to compute, \( T = r^2 \pmod{n} \), so that \( 1 < r < n-1 \).
- Victor, the verifier, selects a random number \( d \) and sends it to Peggy so that \( 1 < d < v-1 \).
- Peggy computes \( D = r \times b^r \) and sends it to Victor.
- Victor, the verifier, computes \( T' = D^2 \times J^d \pmod{n} \), if \( T = T' \pmod{n} \), then the verification succeeds.

Zero-Knowledge Proofs of Identity Based on Elgamal on Conic: In 2004, a new scheme of zero-knowledge proofs of identity based on Elgamal on conic was proposed [13]. The security of this scheme is based on discrete logarithm problem on conic over finite fields. Compared with previous zero-knowledge schemes which use elliptic curve, the design and implementation of this scheme is easier. The protocol of this scheme takes the form a three-way protocol (Figure 3) and works as the following:

Initial Parameters: Peggy chooses a random integer \( \alpha \in \{1,2,\ldots,p\} \) as her private key and \( (C, P, aP) \) as her public key after computing \( aP \), where \( p \) is a prime number (except 2).

The Protocol Steps:

- Peggy chooses a random integer \( k \), then computes \( x = a(kP) \) and sends \( x \) to Victor.
- Victor generates a random bit \( b \). If \( b = 0 \) then \( M = 0 \); else Victor generates a random integer \( i \) and sets \( M = iP \); Victor sends both \( b \) and \( M \) to Peggy.
- If \( b = 0 \), Peggy sends \( k \) to Victor; or else Peggy computes \( Y = a(M) \) and sends \( Y \) to Victor.
- If \( b = 0 \), Victor verifies if \( X \) is equal to \( k(aP) \) and believes that Peggy knows the value of \( k \). If \( b = 1 \), Victor verifies if \( Y \) is equal to \( i(aP) \). Therefore, he is convinced that Peggy knows the value of \( a \) or not.

In this scheme, the prover and verifier select the number of iteration \( T \). As a result, the value of this parameter (\( T \)) affects the speed and security degree of the scheme if it istoo big or too small. The iteration is done mathematically.
Visual Zero-Knowledge Proof of Identify Scheme: In 2010, Jaafar and Samsudin proposed a visual zero-knowledge proof identity scheme [14] which merged the concept of visual cryptography for binary (black-and-white) images and the concept of zero-knowledge proof of identify. The Visual Zero-Knowledge proof of identity scheme has the advantages of both visual cryptography and Zero-Knowledge. The Visual zero-knowledge proof of identity scheme consists of three phases:

Initialization Phase:
- The prover (or Peggy) and the verifier (or Victor), agree on a public integer random modulus, \( p \).
- The prover (or Peggy) generates her public share \( Pu \).

\[ Pu = [H(Pri || Rnd)]^{-1} \times [Rnd]^{-1} \mod p \]  

(1)
To generate the public share we first need to generate the random and the hash share. To generate the hash share we pad each pixel in the private share with the corresponding pixel in the random share as follows:

\[ hash \ share = H (Priv || Rnd) \]  

(2)

The hash function used is referred to as Pearson's Hash, which is modified to be appropriate for use in the proposed method. In this hash function, there are no shifts or XOR operations. It uses an auxiliary array to produce a single byte as output and the input is any number of bytes. The output depends greatly on every byte of the input string.

Proving Phase: In this phase, the first part entails the prover attempting to prove himself/herself to the verifier. The second part involves the verifier who verifies the prover information. Based on this, we can divide the proving phase into four steps:

- The prover, (Peggy) who intends to prove herself to the verifier, sends her public share to the verifier, (Victor).
- The prover, (Peggy) receives verification/challenge image \( Ch \) from the verifier, (Victor).
- The prover, (Peggy) calculates response share \( Y \).

\[ Y = [H(Pri || Rnd))]^2 \times Ch \times [Rnd]^2 \mod p \]  

(3)
The prover, (Peggy) sends response share $Y$ to the verifier, (Victor).

Verifying Phase: In this phase the verifier attempts to verify the information that has been sent from the prover. To do this, the verifier, (Victor), must take the following steps:

- The verifier, (Victor) receives the response share $Y$ from the prover, (Peggy).
- The verifier calculates $Ch'$ as follows:

$$Pu \times Y \mod p = Ch'$$

(4)

The verifier checks visually if $Ch = Ch'$. If that is true, then the verification process is a success.

Security Analysis: Most of the steps in the proposed scheme depend on a hard mathematical problem which is difficult to cryptanalyze.

$$Pu = [H(Pri || Rnd)]^{-2} \times [Rnd]^{-1} \mod p$$

(6)

Equation 6 is used to generate the public key which the prover sends to verifier. If an eavesdropper intercepts it, he cannot reverse this equation to recalculate what the secret information is, since to do so would require finding
Pri: Peggy’s private share, Rnd: Random share H: Hash function
Ch: challenge image, Y: Peggy’s response share
Fig. 5: The proposed scheme protocol

a multiplicative inverse over a prime field, as well as inverting a hash function based on a given hash digest. This is the same when generating the response share (Equation 7)

\[ Y = [H(Pri || Rnd)]^2 \times Ch \times [Rnd]^2 \mod p \] (7)

In Equation 8, it is possible to recover the challenge share Ch. However, if the challenge share is recovered, it becomes difficult to invert the equation in order to produce the secret information. Moreover, dealing with images makes penetration more difficult. The verifying phase is based on the following equation:

\[ Pu \times Y \mod n = Ch' \] (8)

The second level of the security is based on visual cryptography, which implies that we use the shares in the proposed scheme. Using the shares make the new zero-knowledge less complex in the proposed scheme. In this scheme a very large numbers of pixels increase the level of security even more.

In the event of attack, the attacker will take a long time to extract the secret information since each pixel is composed of three colors R (red), G (green) and B (blue) - 8 bits-per color, which give \(2^8 = 256\) possibilities per pixel, per color. The number of possibilities per pixel is therefore \((2^8)^2 = 2^{24} = 16,777,216\). By using a small image with \(10 \times 10\) pixel, the number of possibilities for the whole image becomes \((2^{24})^{100}\) possibilities. If \(32 \times 32\) pixel is used, the number of possibilities of the whole image becomes...
Table 4: Comparison between existing zero-knowledge proof of identity schemes with the proposed scheme

<table>
<thead>
<tr>
<th>Scheme name</th>
<th>FFS</th>
<th>VZNPIS</th>
<th>The proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Iteration</td>
<td>Many</td>
<td>One</td>
<td>One</td>
</tr>
<tr>
<td>Verification</td>
<td>Mathematically</td>
<td>Visually (limited)</td>
<td>Visually</td>
</tr>
<tr>
<td>Secret Information</td>
<td>Numbers</td>
<td>Noisy images</td>
<td>Noisy images</td>
</tr>
<tr>
<td>Complex computation</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Type of images</td>
<td>None</td>
<td>Black-and-white</td>
<td>Color images</td>
</tr>
<tr>
<td>Security</td>
<td>Large prime number</td>
<td>OR operation</td>
<td>Mathematic hard problem and hash function</td>
</tr>
</tbody>
</table>

Fig. 6: Execution time comparison between the proposed scheme and FFS

Fig. 7: Execution time comparison between the proposed scheme and VZNPIS

(2^{24469000}) possibilities. For an image with pixel size 800 × 600, the number of possibilities of the whole image is (2^{24469000}) possibilities, which makes brute force extremely hard. Note that the number of possibilities mentioned here is huge considering the fact that there are less than 2^{280} atoms in the universe.

For the third level of these security measures, the hash function is used in the proposed scheme. The prover sends the hash value of the private share. He does not need to send his private share. By using a hash function, it is extremely hard for an adversary to calculate the private share from the hash digest.

Performance Analysis of The Proposed Scheme Compared with The Well-Known Proposal Scheme: The proposed protocol has some advantages compared to the traditional zero-knowledge proof of identity schemes. A summary of the comparison is shown in Table 4.

When the proposed scheme is compared with Feige-Fiat-Shamir Zero-Knowledge proof of identity scheme the proposed scheme show better performance. The bar graph in Figure 6 shows that the proposed scheme is faster than the Feige-Fiat-Shamir Zero-Knowledge proof of identity scheme. However, with small size images, the security of the proposed scheme decreases because the image size 5×5 pixel contains 600 bits divided into 25 separate pixels, which will decrease the level of security. If the image size used in the new scheme is more than 300×300 pixels, the new scheme is still faster compared to the Feige-Fiat-Shamir Zero-Knowledge proof of identity and, at the same time, provides a reasonable level of security.

The bar chart in Figure 7 compares the execution time of the Visual Zero-Knowledge proof of identity scheme by using color images against VZNPIS with image size 300 × 300 pixels.
Figure 7 demonstrates that the proposed scheme takes more time than the VZNPIS. By using image size 300 × 300 pixels, the execution time of the proposed scheme is 6.107 seconds, while the execution time of VZNPIS is 4.777 seconds; this means that there is no significant difference between the two schemes. VZNPIS is faster than the proposed scheme because VZNPIS works only with black and white images, which means it deals with only one bit at a time.

The performance analysis shows that of the three schemes, only the proposed scheme works with any type of image and with visual verification. By comparison FFS verification is performed mathematically and VZNPIS verification is performed visually; however the verification share is completely black.

CONCLUSIONS

In this paper the literature has been explored in two parts. The first part provided an overview of existing visual cryptography schemes, while the second part provided an overview of zero-knowledge proof identity schemes, which are related to the work in this research.

This paper proposes a new Zero-Knowledge proof of identity scheme which is a visual zero-knowledge proof of identity scheme using color images. The performance and security analyses of the Visual Zero-Knowledge proof of identity scheme using color images were performed and discussed in this paper. The results of the security analysis showed that the proposed scheme depends on a hard mathematical problem which is difficult to attack. The proposed scheme also uses reasonably large images to provide the needed security. In addition the proposed scheme utilizes random oracle in the form of a hash function which makes recovering the private key close to impossible.

The performance analysis showed that the proposed scheme is faster than the Fiat-Shamir zero-knowledge proof of identity, but slower than VZNPIS. Nonetheless, the results show that, the proposed scheme is a valuable alternative to existing zero-knowledge schemes where the verification procedure can be performed visually. Furthermore, while VZNPIS works only with black-and-white images, the proposed scheme can work with any type of images (color images, noisy images, black and white images, full black images and a full white image).

REFERENCES